(12) UK Patent Application (19) GB (11) 2 332 962 (13) A

(43) Date of A Publication 07.07.1999

(21) Application No 9822722.6

(22) Date of Filing 19.10.1998

(30) Priority Data
(31) 97080560 (32) 31.12.1997 (33) KR

(51) INT CL[6]
G06F 11/14

(52) UK CL (Edition Q)
G4A AAP AME

(56) Documents Cited
GB 2231418 A EP 0858031 A1 US 5559960 A
US 5367682 A

(58) Field of Search
UK CL (Edition Q) G4A AAP AME
INT CL[6] G06F 1/00 11/00 11/14
Online: WPI

(71) Applicant(s)
Samsung Electronics Co Limited
(Incorporated in the Republic of Korea)
416 Maetan-dong, Paldal-gu, Suwon-city,
Kyungki-do, Republic of Korea

(72) Inventor(s)
Hye-Jeong Nam

(74) Agent and/or Address for Service
Dibb Lupton Alsop
Fountain Precinct, Balm Green, SHEFFIELD, S1 1RZ,
United Kingdom

(54) Abstract Title
Backup of booting and FAT information for virus recovery

(57) Both booting information required to boot a hard disc drive and the file allocation table (FAT) are backed up 19 in the maintenance area 1 of the disc, which area is inaccessible to the virus. Hence the working versions of the booting information and FAT, which both reside in the working area 2, may be restored from uninfected versions periodically backed-up in the backup area 19. Backup may alternatively occur during initial booting.

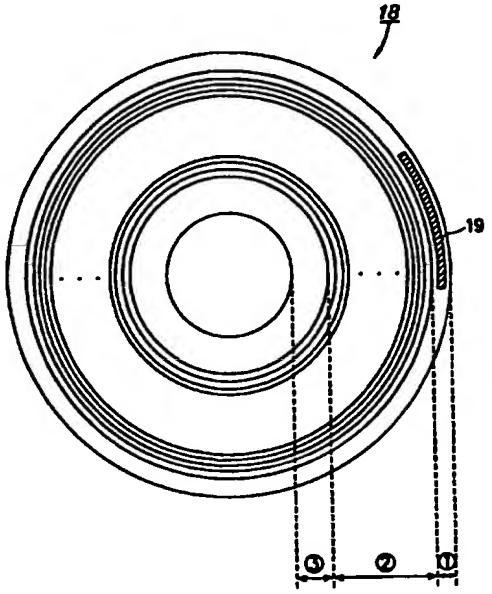

FIG. 2

GB 2 332 962 A

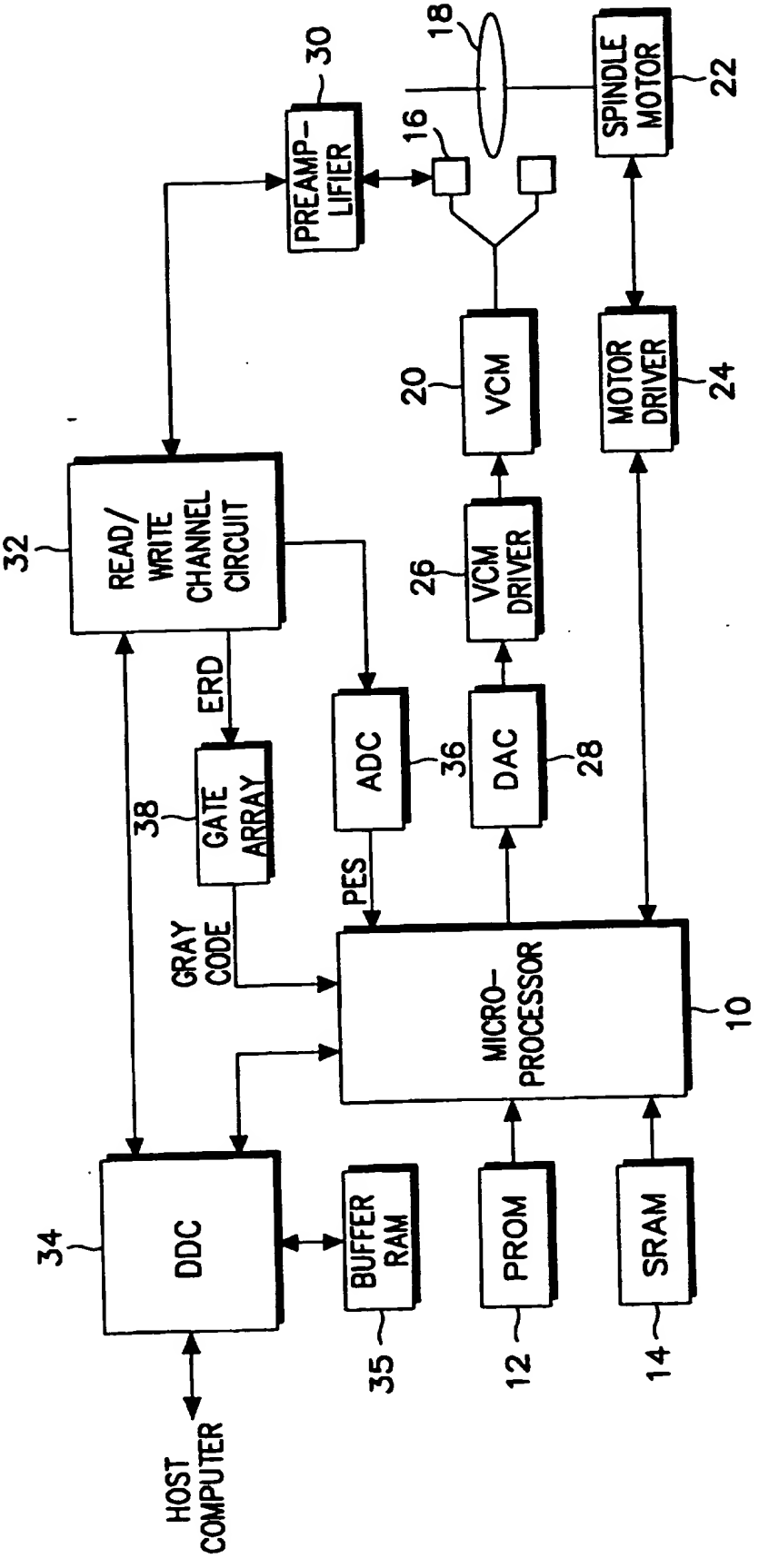
HOST COMPUTER
34
DDC
35
BUFFER RAM
12
PROM
14
SRAM
10
MICRO-PROCESSOR
GRAY CODE
38
GATE ARRAY
ERD
32
READ/ WRITE CHANNEL CIRCUIT
PES
36
ADC
28
DAC
26
VCM DRIVER
20
VCM
30
PREAMP-LIFIER
16
18
SPINDLE MOTOR
22
MOTOR DRIVER
24

FIG. 1

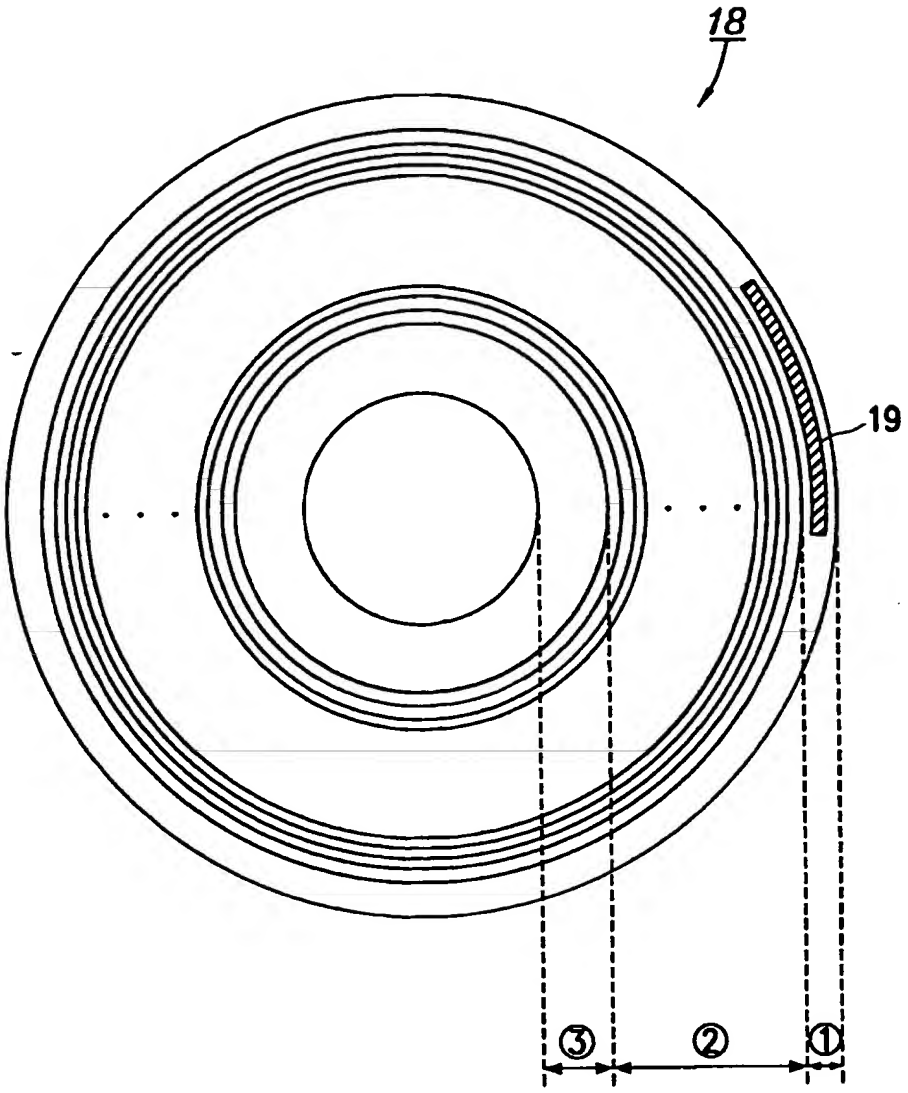

FIG. 2

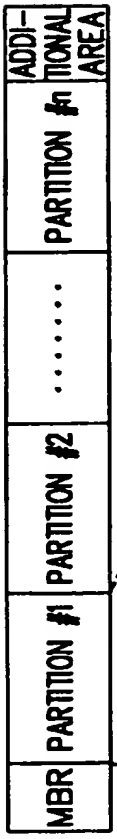
MBR
PARTITION #1
PARTITION #2
.....
PARTITION #n
ADDI-
TIONAL
AREA

FIG. 3A

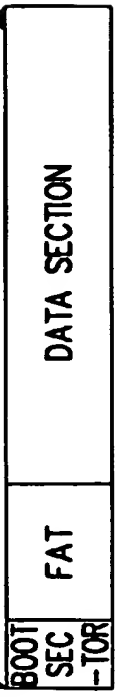
BOOT
SEC
-TOR
FAT
DATA SECTION

FIG. 3B

DATA PROCESSING METHOD AND SYSTEM

The present invention relates to a hard disk drive, and in particular, to a method of additionally providing the function of restoring data damaged by a computer virus in a hard disk drive.

In a hard disk drive, widely used as an auxiliary memory device for a computer system by virtue of its high data storage capacity, data is magnetically recorded on a magnetic disk (referred to as a disk, hereinafter). The hard disk drive has been increasingly used as personal computers (PCs) have proliferated.

Along with the increased provision and use of computers to general users, viral damage has also increased, including loss of stored data or shut-down of a computer system by a computer virus (hereinafter, referred to as a virus).

More specifically, a virus is a kind of software program that operates in relation to computer memory, storage devices, data and software and is stored in a file like a general program. The virus gives rise to many problems such as changing or erasing an existing file or the structure of a system, damaging data, destroying program files by re-formatting the or a hard disk, and locking-up the computer. The virus can also reproduces itself in another disk or computer.

A disk is infected with a virus by copying a virus-infected file or simply by viewing the file directory of the file in some cases.

To restore such a virus-infected disk, a so-called vaccine program has emerged for removal of the virus and recovery of damaged data. However, the kinds of viruses are increasing due to the increased use of computers, and the viruses act more subversively. Under these circumstances, it is impossible to cope with the viruses with vaccine programs for protecting data against viral damages.

An object of the present invention is to provide a method of

restoring data damaged by a virus in a hard disk drive.

Accordingly, a first aspect of the present invention provides A data processing method for restoring data stored on a storage medium of a data storage device in the event of damage by a computer virus, the method, comprising the steps of: backing up system information of the storage device into a predetermined area inaccessible to the computer virus.

Once virus damaged has been sustained, it will be necessary to recover the state of the disk prior art the virus damage. Accordingly, an embodiment provides a method further comprising the steps of restoring the system information from the backed up system information when the system information has been infected with the computer virus.

Critical information which could readily render a disk unusable may be the system information. Therefore, preferably, an embodiment provides a method wherein the system information includes booting information required to boot the hard disk drive. Preferably, a method is provided wherein the booting information is master boot record (MBR) and information in a boot sector.

Still further, an embodiment provides a method wherein the system information includes file position information indicating the position of a file on the disk. In the event that the latest version of the position information, eg FAT table, has been damaged and a damaged version of the position information has been stored in the predetermined area, an embodiment of the present invention provides a method wherein the file position information backed up into the predetermined area comprises the latest file position information and at least one previous file position information. Preferably, an embodiment provides a method wherein the file position information includes a file allocation table (FAT).

Since a virus may strike at any time without warning during the operation of a computer, an embodiment provides a method wherein the system information is backed up into the predetermined area is updated if at least one predetermined condition has been satisfied.

Preferably, the predetermined condition is the initial booting of the storage device. Additionally or alternatively, the predetermined condition may be the elapse of a predetermined period of time.

Preferably, a method is provided wherein the predetermined area of the disk is a maintenance area of the disk.

A second aspect of the present invention provides a data storage device comprising a data storage medium, the device, comprising means for backing up system information of the storage device into a predetermined area of the storage medium inaccessible to a computer virus.

Preferably, the data storage device further comprising means for restoring the system information from the backed up system information when the system information has been infected with the computer virus.

Advantageously, the present invention allows the correct operation of a storage medium to be restored in the event of damage by a virus and particularly, provides a method of restoring a system and a file recorded on a disk, which can not be booted and read, respectively, due to the virus. This affords greater protection for user data and increase the reliability of a hard disk drive by reducing rapidly increasing viral damages.

An embodiment provides a method of restoring data damaged by a computer virus on a magnetic information recording disk in a hard disk drive. In the data restoring method, booting information required to boot the hard disk drive and file position information indicating the position of a file when data is stored in a file unit are backed up in a predetermined portion of a maintenance area on the disk. The booting information or the file position information is restored based on the backed up information when the booting information or the file position information has been infected with a computer virus.

Advantageously, the microprocessor 10 in the hard disk drive as constituted above is able to restore data damaged by a virus.

Embodiments of the present invention will now be described, by way of example only, with reference to the accompanying drawings in which:

figure 1 is a block diagram of a hard disk drive to which the present invention is applied;

figure 2 is an exemplary format diagram of an information recording disk shown in figure 1; and

figures 3A and 3B are detailed format diagrams of a data area shown in 3.

A preferred embodiment of the present invention will be described in detail. While details such as a method of storing a file allocation table (FAT) are disclosed, they are mere exemplary applications for a comprehensive understanding of the present invention. Thus, it is clearly understood that many modifications can be made to these details by anyone skilled in the art within the scope and spirit of the present invention.

The operation of a hard disk drive will be first described. Figure 1 is a block diagram of a hard disk drive to which the present invention is applied. Referring to figure 1, a microprocessor 10 is connected to a PROM (Programmable Read Only Memory) 12 for storing a specific control program and data of the microprocessor 10, and an SRAM (Static Random Access Memory) 14. The microprocessor controls the whole operation of the HDD. A head 16, fixed at an end of an actuator, horizontally flies over a rotating disk 18 for writing or reading data to or from the disk 18. A VCM (Voice Coil Motor) 20, positioned at the other end of the actuator, drives the head 16 according to the level and direction of a current applied to the VCM 20. A spindle motor 22 rotates the disk 18 stacked around a drive shaft according to a control signal received from a motor driver 24. A VCM driver 26 is connected to the VCM 20 and controls the driving of the VCM 20. A DAC (Digital-to-Analog Converter) 28, connected to the microprocessor 10 and the VCM driver 26, receives a digital control signal from the microprocessor 10, converts the received signal to an analog signal, and outputs the analog signal to the VCM driver 26.

The motor driver 24 is connected to the spindle motor 22 and the microprocessor 10, for controlling the driving of the spindle motor 22

under the control of the microprocessor 10. A preamplifier 30 is connected to the head 16, pre-amplifies a reproduced signal, and outputs an write signal to the head 16 or receives a read signal from the head. A read/write channel circuit 32 connected to the microprocessor 10, the preamplifier 30, and a DDC (Disk Data Controller) 34, receives write data from the DDC 34, encodes the write data, and outputs the encoded write data to the preamplifier 30 under the control of the microprocessor 10. The read/write channel circuit 32 converts an analog reproduction signal received from the preamplifier 30 to a digital signal, and outputs the digital signal as encoded read data ERD. An ADC (Analog-to-Digital Converter) 36 connected to the read/write channel circuit 32, receives an analog servo reproduction signal from the read/write channel circuit 32, converts the received signal to a digital position error signal PES, and outputs the signal PES to the microprocessor 10. A gate array 38 connected to the read/write channel circuit 32, receives the signal ERD, detects servo information such as a gray code in a servo area of the disk 18, and outputs the detected servo information. The DDC 34 has a sequencer for operating according to a microprogram downloaded from the microprocessor 10, and records data received from an external data input device (e.g., a host computer) on the disk 18 via the read/write channel circuit 32 and the preamplifier 30. The DDC 34 also reads the data from the disk 18 and transmits the read data to the external data input device. The DDC 34 acts as a communication interface between the host computer and the microprocessor 10, and temporarily stores data transmitted between the host computer and the microprocessor 10 and between the host computer and the read/write channel circuit 32 in a buffer RAM 35.

The microprocessor 10 for controlling the whole operation of the drive controls the DDC 34 in response to a read or write instruction received from the host computer, and controls track seek and track following. The PROM 12 stores the operation program of the microprocessor 10 and various designated values.

According to the feature of the present invention, the microprocessor 10 backs up data which will cause serious problems if it is damaged by a virus infecting data recorded on the disk 18, that is,

system booting information and a FAT including the titles and positions of recorded data files in a maintenance area inaccessible to a general user.

Figure 2 is a format diagram of a general information storing disk 18 divided into several areas. Referring to Figure 2, the disk 18 is largely divided into a system area ①, a data area ②, and a parking zone ③.

The system area ① also called a maintenance area is inaccessible to a general user, and is used for storing system data and data used to repair and maintain a hard disk drive. The data area ② accessible to the general user, is for storing general user data. The parking zone ③ is the place where a magnetic writing/reading device (i.e., head, not shown) for recording data onto and reading data from the disk 18 is parked, and has no data recorded therein.

As for the system area ①, a hard disk drive manufacturer records various pieces of system-related information in the maintenance area ① of a disk, such as the specific number of a drive, fabrication-related information, defect-log-in data, a defect list, or SMART (Self Monitoring Analysis Reporting Technology), and reads them when necessary. As the information recorded in the maintenance area ① is unique to the drive, it cannot be stored in a ROM and is read out to a RAM of the drive when necessary. One to four tracks are usually assigned to the maintenance area ①.

According to an embodiment of the present invention, information which is likely to cause serious problems if it is damaged by a virus among pieces of information recorded on the disk 18 is stored beforehand in a predetermined portion 19 of the maintenance area ①. The information may include system booting information and a FAT having the titles and positions of recorded data files. If such information is damaged by a virus, the system cannot be booted successfully. If the position information of a recorded file is damaged, file data cannot be restored even if the system is booted. For these reasons, the system booting information and the FAT are often targets of a virus attack. When a data file is damaged by a virus, the file is partially

or wholly damaged. However, possible damage of the system booting information and the file position information causes the serious problem that the data of all files recorded on a disk is inaccessible. Therefore, the booting information and the file position information are backed up in a safe area, that is, the maintenance area, so that existing information can be restored from the backed-up information in the event of damage.

The booting information and the file position information are generally stored in the data area ②, which will be described in detail with reference to the attached drawings.

Detailed format diagrams of the data area ② for storing data are shown in figures 3A and 3B. As shown in figure 3A, the data area ② is divided into several partitions. This is referred to as partitioning to store at least one operating system on one disk. A partition table having the position of each partition, that is, the starting and ending positions of each partition is generally positioned in sector #1 of cylinder #0 in head #0 usually called MBR (Master Boot Record), as shown in figure 3A. The MBR has information of each partition and, especially, information of a partition including a boot program of a present operating system for booting a hard disk drive.

In the DOS (Disk Operating System), the boot program is generally stored in the first sector of the first partition following the MBR, that is, of partition #1 in figure 3A.

A detailed format diagram of partition #1 is shown in figure 3B. Referring to figure 3B, the area having the boot program is generally called a boot sector. The boot sector occupies exactly one sector and is provided in the first sector of the partition.

When a drive is booted by turning on a computer, the microprocessor 10 sequentially seeks sector #1 of cylinder #0 on head #0 of the disk 18, reads the MBR information stored in the sector, seeks a partition having a boot program, searches for a boot sector of the corresponding partition, reads out the boot program to the SRAM 14, and implements a booting operation. Therefore, information recorded in

the MBR and the boot sector is necessary for the booting operation, as described above.

In figure 3B, a FAT follows the boot sector and indicates the position of information stored in file units in a data area of the disk 18, from a user's point of view. The FAT also stores information relating to data clusters which is a set of several sectors, and has information relating to damaged clusters and empty clusters so that it can indicate which empty cluster to use when a new file is recorded and prevent file data from being recorded in a damaged cluster. The FAT is modified when a user stores a new file, changes an existing file, or erases the existing file.

After a drive has been manufactured by a drive manufacturer, the above MBR, boot sector, and FAT are backed up in the predetermined portion 19 of the maintenance area ①. The MBR and the boot sector are valid unless the hard disk drive is newly initialized, whereas the FAT is continuously modified. Therefore, the FAT should be updated periodically. In the embodiment of the present invention, the FAT is updated whenever the computer system is turned on. To prevent the FAT stored in the predetermined portion 19 of the maintenance area ① from being updated according to an FAT damaged by a virus, space is prepared beforehand for at least two FATs in the predetermined portion 19 of the maintenance area ①, and the latest FAT and at least one previous FAT can be stored in the space.

If file position information is damaged by a virus or a drive cannot be booted, a drive manufacturer issues an instruction to the microprocessor 10 to restore an MBR, a boot sector, and an FAT damaged by a virus by means of the MBR and the boot sector stored in the predetermined portion 19 of the maintenance area ①, and an uninfected FAT selected from among several FATs. This instruction is unique to each drive. Upon receiving the instruction, the microprocessor 10 restores data, especially, the MBR, boot sector, and FAT damaged by the virus.

According to the present invention as described above, system booting information and an FAT having the titles and positions of

recorded data files, which are likely cause a serious problem when they are damaged by a virus among various pieces of information recorded on an information recording disk in a hard disk drive, are backed up in a maintenance area inaccessible to a general user for use in restoring system booting information and an FAT when they have been infected with a virus. Therefore, the effects of viral damage to a hard disk drive are reduced, user data is protected, and the reliability of the drive is increased.

CLAIMS

1. A data processing method for restoring data stored on a storage medium of a data storage device in the event of damage by a computer virus, the method, comprising the steps of: backing up system information of the storage device into a predetermined area inaccessible to the computer virus.

2. A method as claimed in claim 1, further comprising the steps of restoring the system information from the backed up system information when the system information has been infected with the computer virus.

3. A method as claimed in either of claims 1 or 2, wherein the system information includes booting information required to boot the hard disk drive.

4. A method as claimed in claim 3, wherein the booting information is master boot record (MBR) and information in a boot sector.

5. A method as claimed in any preceding claim, wherein the system information includes file position information indicating the position of a file on the disk.

6. A method as claimed in claim 5, wherein the file position information backed up into the predetermined area comprises the latest file position information and at least one previous file position information.

7. A method as claimed in either of claims 5 or 6, wherein the file position information includes a file allocation table (FAT).

8. A method as claimed in preceding claim, wherein the system information is backed up into the predetermined area is updated if at least one predetermined condition has been

satisfied.

9. A method as claimed in claim 8, wherein the predetermined condition is the initial booting of the storage device.

10. A method as claimed in either of claims 8 or 9, wherein the predetermined condition is the elapse of a predetermined period of time.

11. A method as claimed in any preceding claim, wherein the predetermined area of the disk is a maintenance area of the disk.

12. A data storage device comprising a data storage medium, the device, comprising means for backing up system information of the storage device into a predetermined area of the storage medium inaccessible to a computer virus.

13. A device as claimed in claim 12, further comprising means for restoring the system information from the backed up system information when the system information has been infected with the computer virus.

14. A device as claimed in either of claims 12 or 13, wherein the system information includes booting information required to boot the hard disk drive.

15. A device as claimed in claim 14, wherein the booting information is master boot record (MBR) and information in a boot sector.

16. A device as claimed in any of claims 12 to 15, wherein the system information includes file position information indicating the position of a file on the disk.

17. A device as claimed in claim 16, wherein the file position information backed up into the predetermined area

comprises the latest file position information and at least one previous file position information.

18. A device as claimed in either of claims 16 or 17, wherein the file position information includes a file allocation table (FAT).

19. A device as claimed in any of claims 12 to 18, wherein the system information is backed up into the predetermined area is updated if at least one predetermined condition has been satisfied.

20. A device as claimed in claim 19, wherein the predetermined condition is the initial booting of the storage device.

21. A device as claimed in either of claims 19 or 20, wherein the predetermined condition is the elapse of a predetermined period of time.

22. A device as claimed in any of claims 12 to 21, wherein the predetermined area of the disk is a maintenance area of the disk.

23. A data processing method substantially as described herein with reference to and/or as illustrated in the accompanying drawings.

24. A data storage device substantially as described herein with reference to and/or as illustrated in the accompanying drawings.

The Patent Office

INVESTOR IN PEOPLE

Application No:	GB 9822722.6	**Examiner:**	K. Sylvan
Claims searched:	1-24	**Date of search:**	11 March 1999

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.Q): G4A (AAP,AME)

Int Cl (Ed.6): G06F (1/00,11/00,11/14)

Other: Online: WPI

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
A	GB2231418 A	S&S Enterprises. See abstract.	-
A	EP0858031 A1	IBM. See abstract.	-
A	US5559960	Lettvin. See abstract.	-
A	US5367682	Chang. See abstract.	-

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.